REMARKS

Claims 1-3, 5-11 and 13-28 are currently pending in the subject application and are presently under consideration. Claims 1, 14, 18, 22, 26 and 27 have been amended as shown on pages 2-7of the Reply. Claim 13 has been cancelled herein. New claim 28 has been added. Support for the amendments can be found at page 2, ll. 8-13 page 10, line 4 to page 16, line 6, page 16 lines 1-3 and page 17 lines 20-27.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-5, 9, 10 and 12-27 Under 35 U.S.C. §102(b)

In the Final Office Action dated November 21, 2007, claims 1-5, 9, 10 and 12-27 stand rejected under 35 U.S.C. §102(b) as being anticipated by Stallings, William. (Cryptography and Network Security; Third Edition. Chapter 9/Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems. Upper Saddle River, NJ. Prentice Hall, 2003. Pgs. 259-265, 290-293, 444 and 655). Withdrawal of this rejection is requested for the following reasons. The cited reference fails to disclose or suggest all aspects set forth in the subject claims.

> A single prior art reference anticipates a patent claim only if it ***expressly or inherently describes each and every limitation set forth in the patent claim***. *Trintec Industries, Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The ***identical invention must be shown in as complete detail as is contained in the ... claim***. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

The claimed invention provides methods and systems facilitating the exchange and use of a session key to facilitate secure communication. To this end amended independent claim 1 recites *a message encryption system comprising: a session key employed to securely exchange a message associated with a dialog; and, an encryption component that employs asymmetric encryption to first securely transmit the session key, the session key thereafter being employed to encrypt the message and securely exchange the message, wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the*

message, ***the message is employed as part of a service broker security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service***. Independent claims 14, 18, 22, 26 and 27 recite similar features. Stallings is silent regarding such novel aspects.

Stallings relates to principles of public-key cryptosystems and secret key distribution with confidentiality and authentication. At the cited portions, Stallings discloses a secret key distribution that provides protection against both active and passive attacks. A secret key is encrypted using the private key-public key pair and passed from an initiator to a recipient. The encrypted message containing the secret key is decrypts the message to recover the secret key. Further, Stallings discloses that each session key is associated with a single message and is used for encrypting and decrypting the message. In contrast, the claimed invention allows for encrypting messages sent from the initiator, first with the session key then encrypted message again encrypted with the private key of the initiator. This message is employed by a service broker security system that facilitates location transparency of services. The initiator and target have a copy of each other's public key and with appropriate permissions to send to services, they will be able to access the service regardless of where the service is actually located. However, Stallings is silent regarding ***the message is employed as part of a service broker security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service*** as recited by the subject claims.

By allowing services to be addressed logically by name, the system and method of the present invention allow applications to be built independent of where the service is located physically. At deployment time, the services can be moved to different physical locations without affecting the application.

Additionally Stallings fails to teach or suggest running multiple instances of a service in order to balance load on a server running such a service as recited in independent claim 22. All the multiple instances of the service can be associated with a private key of the owner of the service so that any application/subscriber utilizing the service can deal with all the multiple instances as a unit. Further, each of the instances can negotiate a unique session key with their respective accessing applications/subscribers.

In view of at least the foregoing, it is clear that an identical invention as recited in the subject claims is not taught or suggested by the cited document. Accordingly, it is requested that this rejection with respect to independent claims 1, 14, 18, 22, 26 and 27 should be withdrawn.

II. Rejection of Claim 11 Under 35 U.S.C. §103(a)

In the Final Office Action dated November 21, 2007, claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings. It is respectfully requested that this rejection be withdrawn for at least the following reasons. Claim 11 depends from independent claim 1. As discussed supra, Stallings does not teach or suggest all aspects of amended independent claim 1. Accordingly, it is requested that this rejection be withdrawn.

III. Rejection of Claims 6-8 Under 35 U.S.C. §103(a)

In the Final Office Action dated November 21, 2007, claims 6-8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings in view of VanHeyningen *et al.* (US 2002/0112152). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Stallings and VanHeyningen *et al.* do not teach or suggest all aspects set forth in the subject claims. Claims 6-8 depend from independent claim 1, and as discussed supra, Stallings does not teach or suggest all aspects recited by amended independent claim 1. VanHeyningen *et al.* discloses methods and apparatus for providing secure streaming data transmission facilities using unreliable protocols and does not compensate for the aforementioned deficiencies of Stallings. Accordingly, it is respectfully submitted that this rejection should be withdrawn.

IV. New Claim 28

Newly added claim 28 emphasizes novel aspects of the invention discussed supra in connection with claims 1-27. Accordingly, this claim is patentably distinct over the art of record for at least the same reasons as are claims 1-27.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP566US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731